

# NYDFS 500 Cybersecurity Regulation Enforcement Actions

## Causes and Consequences

The webinar will start shortly

# Agenda

- 1 Introductions
- 2 Enforcement Actions
- 3 Causes & Consequences
- 4 Avoiding & Mitigating Penalties
- 5 Q & A

# Introductions



**John Jarrold**

- Security & Risk Management Consultant



**Richard Suls**


- Security & Risk Management Consultant



**Miguel Gutierrez**

- Security & Risk Management Consultant

# Reminder

Name	Comment	 	Submit
------	---------	---	--------

If you have any questions,  
please submit using the  
questions/comment box



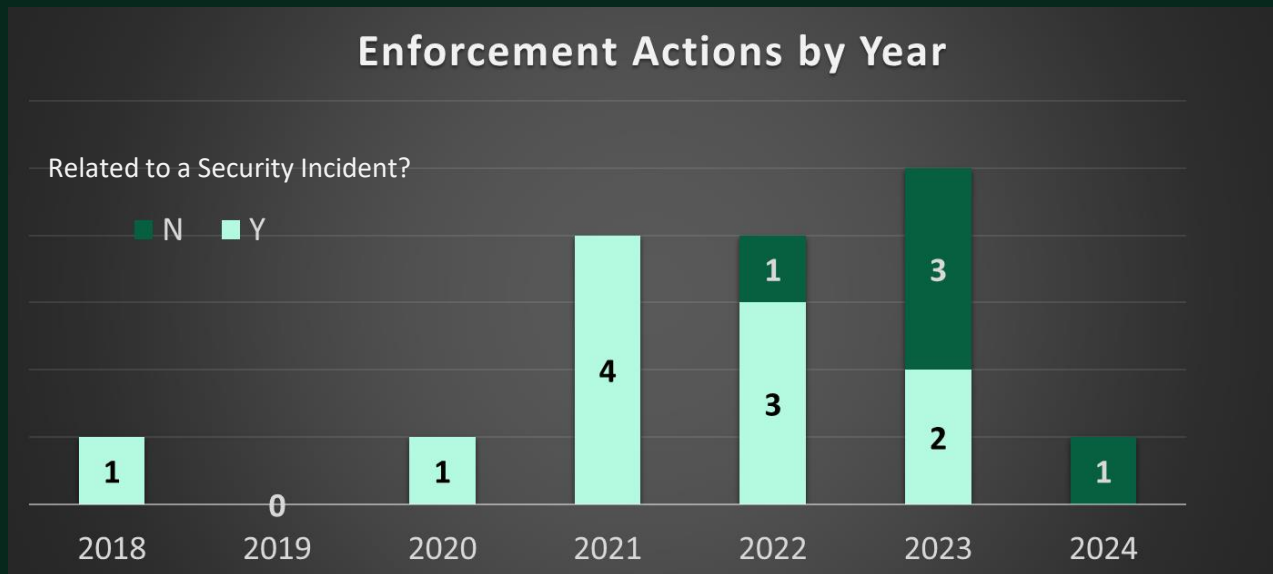
# What are Enforcement Actions?

- Legal measures that NYDFS takes against Covered Entities that violate its regulations
- Generally based on a Consent Order, which is a legally binding agreement between NYDFS and the Covered Entity to resolve the matter without going to trial
- A typical Consent Order:
  - Describes the cyber security incident or deficiencies that led to the action
  - Identifies specific sections of the regulation that were violated
  - Prescribes remedial actions
  - Includes a monetary penalty
- Enforcement actions are public records published on the NYDFS website



# Analysis of Enforcement Actions

- There have been 16 enforcement actions since the regulation was enacted
- The average monetary penalty was almost \$3 million, ranging from \$1M to \$5M
- Security incidents related to enforcement actions resulted in theft over \$1.9M
- Only one Consent Order so far in 2024
- Eleven actions were directly related to security incidents; five were due to deficiencies discovered in exams



# Cybersecurity Events

*And just when it can't get any worse... "NYDFS on Line 2"*

**July 2017**

Threat actors exploited an **unpatched vulnerability** on a webserver to gain unauthorized access to **NPI of 148 million Americans** and 15 British citizens

**September 2018**

**Phishing attack** using a fake O365 login page sent to a large number of employees succeeded in stealing credentials from a number of employees which gave the threat actor **access to consumer NPI**.

**October 2018**

**Phishing attack** used to compromise 15 employee email accounts which were in turn used to launch additional phishing attacks against other employees leading to **exposure of consumer NPI**.

**December 2018**

**Web vulnerability** left more than 850 million documents publicly exposed for multiple years. Some of these documents contained **NPI such as bank account numbers, mortgage and tax records, SSNs, wire transaction receipts, and drivers license images**, which could have been used by an attacker to engage in identity theft or outright theft of consumer assets.

**March 2019**

**Phishing attack** used to steal email account credentials of an employee who regularly handled consumer NPI in processing loan applications.

**September 2019**

**Phishing attack** used to steal employee email credentials. The threat actor then posed as the employee to initiate a **\$35,000 funds transfer**.

**September 2019**

**Phishing attack** used to compromise email account of an employee who had access to consumer NPI. Breach discovered when the threat actor sent an email to HR requesting changes to the employee's direct deposit.

**April 2020**

**Phishing attack or password spray attack** used to compromise 124 employee email accounts. Threat actor then used this access to send additional phishing emails to other employees which resulted in gaining access email attachments containing **NPI, including passport numbers and a small number of SSNs and credit card numbers**.

**April 2020**

Likely **phishing attack** used to compromise a broker's email account. Threat actor then posed as the broker to initiate two **fund transfers** each in the amount of **\$200,000**.

**July 2020**

**Phishing attack** used to gain access to a mailbox which had login credentials shared by nine employees and contained over **six years' worth of consumer NPI**.

**August 2020**

**Ransomware attack** encrypts certain systems and **exfiltrates both consumer and employee NPI**, including some employee SSNs and private health info

**March 2021**

**Phishing attacks** launched from a compromised employee email account

**May 2021**

**Phishing attack** resulted in unauthorized access to approximately 6,000 consumer accounts and **theft of \$1.5 million**.

**June 2021**

**Phishing attack** used to compromise 5 contractor email accounts which were in turn used to launch phishing attacks against customers.

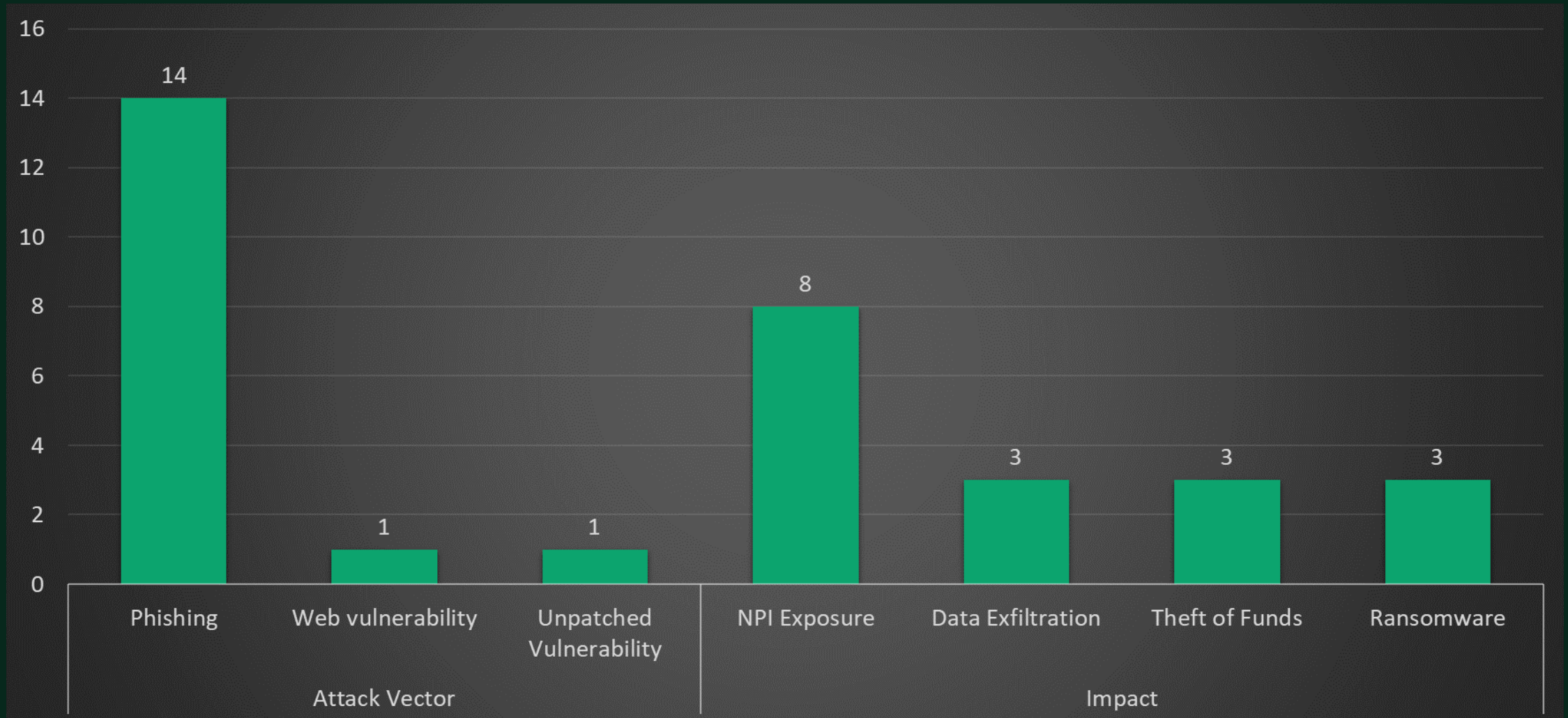
**September 2021**

**Phishing attack** on a network administrator resulted in **ransomware** encrypting 1,800 devices and exfiltration of consumer and employee NPI.



# Attack Vector & Impact

*Surprise, surprise - phishing strikes again*





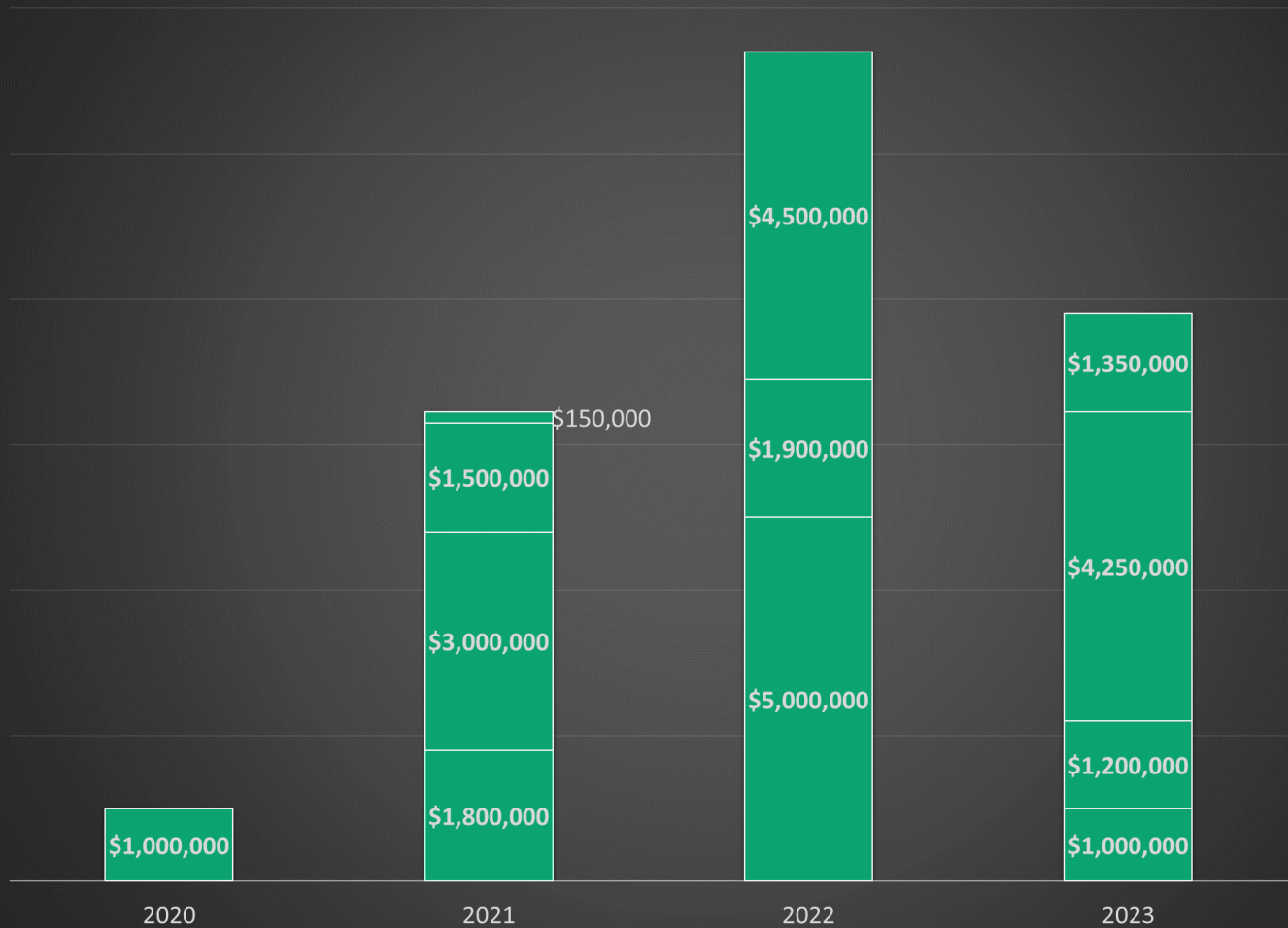
# Violations by Section

*The Enforcement Actions have cited violations of every section of the regulation*

Section	Violations
§500.02 Cybersecurity Program	7
§500.03 Cybersecurity Policy	7
§500.04 Chief Information Security Officer	5
§500.04(a) Chief Information Security Officer	1
§500.04(b) Annual Report to the BoD	4
§500.05 Penetration Testing and Vulnerability Assessments	1
§500.06 Audit Trail	1
§500.07 Access Privileges	4
§500.08 Application Security	1
§500.09 Risk Assessment	2
§500.10 Cybersecurity Personnel and Intelligence	3
§500.11 Third Party Service Provider Security Policy	3
§500.12 Multi-Factor Authentication	8
§500.13 Limitations on Data Retention	2
§500.14 Training and Monitoring	3
§500.15 Encryption of Nonpublic Information	2
§500.16 Incident Response Plan	2
§500.17 Notices to Superintendent	19
§500.17(a) Notice of Cybersecurity Event	5
§500.17(b) Annual Statement of Compliance	14

# Monetary Penalties

Monetary Penalties by Year \*



❖ Note the chart does not reflect the following penalties from Enforcement Actions where cybersecurity violations were combined other areas of non-compliance (e.g. anti-money laundering regulations).

Not Reflected in the Chart:

Year	Penalty
2018	\$19,200,00
2022	\$30,000,000
2023	\$50,000,000
2024	\$8,000,000

# \$500.20(c) Factors for Assessing Penalties

1. The extent to which the covered **entity has cooperated** with the superintendent in the investigation of such acts;
2. The **good faith** of the entity;
3. Whether the violations resulted from conduct that was **unintentional or inadvertent, reckless or intentional and deliberate**;
4. Whether the violation was a result of **failure to remedy previous examination matters requiring attention**, or failing to adhere to any disciplinary letter, letter of instructions or similar;
5. Any **history of prior violations**;
6. Whether the violation involved an **isolated incident, repeat violations, systemic violations or a pattern of violations**;
7. Whether the covered entity provided **false or misleading information**;
8. The extent of **harm to consumers**;
9. Whether required, **accurate and timely disclosures** were made to affected consumers;
10. The **gravity of the violations**;
11. The **number of violations** and the **length of time** over which they occurred;
12. The extent, if any, to which the **senior governing body participated** therein;
13. Any penalty or **sanction imposed by any other regulatory agency**;
14. The **financial resources, net worth and annual business volume** of the covered entity and its affiliates;
15. The extent to which the relevant **policies and procedures** of the company are **consistent with nationally recognized cybersecurity frameworks**, such as NIST; and
16. Such other matters as **justice and the public interest** require.



# Q&A

Name	Comment	 	Submit
------	---------	---	--------

Please submit using the  
questions/comment box





**Thank you for  
attending**

